Claims 11-21 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Hiroya et al. (EP 0848 343 A2). In response, Applicants have amended claims 11, 17, 19, and 21 and canceled claim 18.

Claim 11, as amended, recites the step of:

> receiving, by a second party from a first party, electronic currency for which the first party seeks a refund, wherein the electronic currency includes a first value derived from information identifying the first party **and wherein the second party is unable to identify the first party with the first value**;
>
> receiving, by the second party from the first party, the information identifying the first party and instructions for deriving the first value from the identifying information...

In a typical embodiment, the first party is a consumer and the second party is a vendor. The consumer sends electronic currency to the vendor. Although the currency includes a value derived from an identification of the consumer, the vendor is unable to identify the consumer with it. This arrangement is advantageous because it allows the consumer to spend the currency while remaining completely anonymous to the vendor.

In the case where the consumer is seeking a refund, however, the consumer sends information identifying the consumer to the vendor along with instructions on how to make the identifying information match the value in the electronic currency. The vendor follows the instructions and, if there is a match, knows that the electronic currency was issued to the consumer seeking the refund. Thus, the claimed invention is advantageous because it allows the consumer to be anonymous in purchase transactions, yet allows the vendor to identify the consumer before issuing a refund.

Hiroya discloses an electronic shopping system enabling a refund to a client. In Hiroya's system, a client sends a repayment request to an ordering management server and receives a repayment permit in response. The client then presents the repayment permit to an electronic money payment server. If the client and permit authenticate, the electronic money payment server remits the money to the client (see cols. 11-12 and FIG. 17).

Unlike the claimed invention, Hiroya's system does not allow the consumer to stay anonymous during purchase transactions and yet be positively identified in refund

transactions. Hiroya's system works in one of two modes: completely anonymous or completely identifiable. In the anonymous mode, the client does not provide any identification to the ordering management server or the electronic money payment server. In this situation, the ordering management server issues a receipt to the client that the client can present to the electronic money payment server (see col. 11, line 56 to col. 12, line 5).

In the identifiable mode, the client explicitly identifies itself to the ordering management server when making the repayment request. The ordering management server, in turn, includes the client identification in the repayment permit (see FIG. 18, "Repayment Recipient ID"). The client digitally signs the message presenting the repayment permit to the electronic money payment server and includes a digital certificate. The electronic money payment server compares the client identification in the digital signature (obtained from a third party certificate authority) with the client identification in the repayment permit to verify that the client seeking repayment is the same client to whom the permit was issued (see col. 12, lines 45-49).

Hiroya, therefore, does not disclose the claimed step of receiving electronic currency, "by a second party from a first party," including "a first value derived from information identifying the first party and wherein the second party is **unable** to identify the first party with the first value." In the identifiable mode, the ordering management server is **able** to identify the client from the Repayment Recipient ID it receives from the client. The money payment server receives the digital signature and certificate from the client and is by definition **able** to identify the first party with these values by contacting the certificate authority.

In the anonymous mode, Hiroya does not disclose the step of receiving electronic currency including "a first value derived from information identifying the first party" or receiving "information identifying the first party and instructions for deriving the first value from the identifying information" because no identification takes place. For these reasons, Applicants respectfully submit that claim 11, as amended, is not anticipated by Hiroya.

Claim 17, as amended, recites computer instructions for:

> receiving a request to refund electronic currency, the electronic currency including a value identifying the party to whom the currency was issued;
>
> receiving, **from the party seeking the refund**, identifying information identifying the party seeking the refund **and** values for transforming the information identifying the party seeking the refund into the value identifying the party to whom the currency was issued...

Thus, the party seeking the refund supplies the identifying information and the values for transforming the identifying information into the value identifying the party to whom the currency was issued. No third party certificate authority is involved in the transaction.

In Hiroya's system, however, the party seeking the refund supplies only the repayment permit, the digital signature, and the digital certificate. The electronic money payment server must contact the certificate authority in order to derive the Repayment Recipient ID from the digital signature (see Hiroya's FIG. 1, which illustrates the certificate authority). Without the certificate authority, Hiroya has no way to authenticate the party seeking the refund.

Therefore, Hiroya's system does not receive the values for transforming the information identifying the party seeking the refund from the party seeking the refund, as claimed. Instead, Hiroya's system receives these values from a certificate authority. For this reason, Applicants respectfully submit that claim 17, as amended, is not anticipated by Hiroya.

Claims 1-10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Manasse (US Pat. No. 5,802,497) in view of Hiroya. In response, claim 1 has been canceled and replaced by new claim 22, claims 2 and 7-10 have been canceled, and claims 3-6 have been amended to depend from claim 22.

Claim 22 recites:

> a first system for issuing scrip, the scrip including a value derived from an identification of a recipient of the scrip; and
>
> a second system for receiving the scrip issued by the first system **from a party seeking a refund** and issuing a refund in response thereto, the second system further adapted to receive **from the party seeking the refund** the identification of the recipient of the scrip and information

enabling transformation of the information identifying the recipient of the scrip into the value derived from the identification of the recipient of the scrip, and to utilize the received information to verify that the party seeking the refund is the recipient of the scrip.

Claim 22 recites that the second system receives the scrip, the information identifying the recipient of the scrip, and the information enabling transformation of the information identifying the recipient of the scrip from the party seeking the refund. Applicants submit that Hiroya does not disclose or suggest receiving this information from the party seeking the refund as explained above with respect to claim 17.

As the Examiner acknowledges, Manasse fails to disclose or suggest issuing a refund for scrip. Accordingly, Applicants respectfully submit that a person of ordinary skill in the art would not find it obvious to receive the specified information from the party seeking the refund as claimed in view of Hiroya and Manasse. For this reason, Applicants respectfully submit that claim 22 is allowable over the cited art.

Claims not specifically discussed above are believed allowable by virtue of including the features of their respective base claims. Therefore, Applicants respectfully submit that the application is in condition for allowance and request that it be passed to issue. The Examiner is invited to contact the undersigned by telephone to discuss the arguments raised herein or any other aspects of the application.

Respectfully submitted,
STEVEN C. GLASSMAN *et al.*

Dated: July 3, 2001

By: _____
Brian M. Hoffman, Reg. No. 39,713
Attorney for Applicants
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (415) 875-2484
Fax: (415) 281-1350

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Paragraph on page 1, lines 10 through 13:

This application is also related to U.S. Patent Application Serial No. [<Attorney Docket 3763>] 09/273,240, entitled ENCRYPTING SECRETS IN A FILE FOR AN ELECTRONIC MICRO-COMMERCE SYSTEM, which was filed on the same date as the instant application.

Paragraph on page 2, lines 3 through 9:

Known electronic fund transfer systems generally require a "trusted" third party between the vendor and consumer to authenticate the validity of the electronic funds. The requirement of a third party adds expense to every transaction because of the cost of extra communications and encryption. In addition, current electronic fund transfer networks, e.g., Western Union and Federal Reserve banks, typically require physically secure communications media which [is] are immune to "eavesdropping." Such secure networks are generally not available to consumers at large.

Paragraph on page 4, lines 14 through 23:

The above needs are met by a method and system for electronic commerce that provides relative anonymity for regular purchases but optionally allows the vendor to quickly and easily verify the identity of a consumer seeking a refund. The system includes a broker computer system having a database of [broker] vendor scrips, each vendor scrip representing a form of electronic currency. The system also includes a vendor computer system having a database containing products which may be exchanged for the vendor scrips, the vendor computer system capable of providing vendor scrips. In addition, the system includes a consumer computer system having a user interface whereby a consumer may initiate transactions in the consumer computer system to obtain one or more of the products contained in the database of the vendor computer system.

IN THE CLAIMS:

3. (Amended) The system of claim [2] 22, wherein the [third system] recipient of the scrip is adapted to store one or more nonces utilized to create the value [in the scrip identifying] derived from an identification of the recipient of the scrip.

4. (Amended) The system of claim [1] 22, wherein the first system is adapted to receive [information identifying] the identification of the recipient of the scrip prior to issuing the scrip to the recipient.

5. (Amended) The system of claim 4, wherein the first system is further adapted to hash the [received information identifying] identification of the recipient of the scrip with a nonce and store the hash in the issued scrip as the value derived from the recipient of the scrip.

6. (Amended) The system of claim 5, wherein the received information identifying the recipient of the scrip is a hash of identifying information with a second nonce.

11. (Amended) A method of providing a refund in an electronic commerce system, comprising the steps of:

receiving, by a second party from a first party, electronic currency for which the first party seeks a refund, wherein the electronic currency includes a first value derived from information identifying the first party and wherein the second party is unable to identify the first party with the first value;

receiving, by the second party from the first party, the information identifying the first party and instructions for deriving the first value from the identifying information;

using, by the second party, the instructions for deriving the first value from the identifying information to derive a second value from the provided information identifying the first party;

comparing, by the second party, the second value with the first value; and

enabling, by the second party, a refund for the electronic currency if the first value matches the second value.

17. (Amended) A computer readable medium having computer instructions encoded thereon for directing a computer system to provide a refund in an electronic commerce system, the computer instructions comprising instructions for:

receiving a request to refund electronic currency, the electronic currency including a value identifying the party to whom the currency was issued;

receiving, from the party seeking the refund, identifying information identifying the party seeking the refund and values for transforming the information identifying the party seeking the refund into the value identifying the party to whom the currency was issued;

[verifying] utilizing the received values to verify that the received identifying information matches the value in the electronic currency identifying the party to whom the electronic currency was issued; and

responsive to a positive verification, entitling the party to whom the electronic currency was issued to a refund for the electronic currency.

19. (Amended) The computer readable medium of claim [18] 17, wherein the instructions for receiving values comprise instructions for:

receiving one or more nonces with which the information identifying the party seeking the refund is hashed to produce the value identifying the party to whom the currency was issued.

21. (Amended) The computer readable medium of claim 17 further comprising instructions for:

receiving electronic currency containing a first value identifying the party to whom the currency was issued;

hashing the first value [identifying the party to whom the currency was issued] with a nonce to form a second value identifying the party to whom the currency was issued; and

issuing electronic currency incorporating the second value [identifying the party to whom the currency was issued]; wherein

the received request to refund electronic currency comprises a request to refund the electronic currency incorporating the second value.

22. (New) A system comprising:

a first system for issuing scrip, the scrip including a value derived from an identification of a recipient of the scrip; and

a second system for receiving the scrip issued by the first system from a party seeking a refund and issuing a refund in response thereto, the second system further adapted to receive from the party seeking the refund the identification of the recipient of the scrip and information enabling transformation of the identification of the recipient of the scrip into the value derived from the identification of the recipient of the scrip, and to utilize the received information to verify that the party seeking the refund is the recipient of the scrip.